What is claimed is ;

1. a programmable data processing apparatus, comprising:

   a first storage unit, which stores auxiliary data needed in a encryption algorithm for data processing, wherein, when the encryption algorithm is varied, the auxiliary data stored in the first storage unit can be updated correspondently from outside;

   a reader, coupled to the first storage unit for receiving an index so as to read an auxiliary data from the first storage unit according to the index; and

   a processor, coupled to the reader for receiving a data signal corresponding to the index so as to process the data signal according to the auxiliary data corresponding to the index.

2. The programmable data processing apparatus of claim 1, wherein the encryption algorithm is IEEE802.11i Counter-Mode/CBC-MAC Protocol (CCMP), and the data signal is a portion of MAC Service Data Unit (MSDU) of wireless local area network (WLAN).

3. The programmable data processing apparatus of claim 1, further comprising: a third storage unit coupled to the processor 27, for receiving a processed data signal from the processor, and output the processed signal to a posterior circuit when the processed signal is accumulated to a designated amount of bits

4. The programmable data processing apparatus of claim 3, wherein the designated amount of bits is 128 bits.

5. The programmable data processing apparatus of claim 1, wherein the first storage unit is a read only memory (ROM).

6. The programmable data processing apparatus of claim 1, wherein the first storage unit is a programmable read only memory (PROM).

7. The programmable data processing apparatus of claim 1, wherein the first storage unit is an erasable programmable read only memory (EPROM).

8. The programmable data processing apparatus of claim 1, wherein

the first storage unit is an electrically erasable programmable read only memory (EEPROM).

9. The programmable data processing apparatus of claim 1, wherein the processor further comprising: an initialization device coupled to the reader, which is used for setting partial bits of the data signal to a specified value according to the auxiliary data corresponding to the index.

10. The programmable data processing apparatus of claim 9, wherein the specified value can be one of the following: 0 and 1.

11. The programmable data processing apparatus of claim 1, wherein the processor further comprising: a discard device coupled to the reader, which is used for discarding partial bits of the data signal according to the auxiliary data corresponding to the index.

12. The programmable data processing apparatus of claim 1, wherein the processor further comprising: a format device having a first input for inputting data and a second input for receiving a register signal coming from a second storage unit, wherein the format device will format the first input and the second input according to a process length so as to output a processed signal, moreover, the data exceeding the process length will be send to the second storage unit for registering.

13. The programmable data processing apparatus of claim 12, wherein the second storage unit connecting to the format device of the processor can receive a preload signal and the data exceeding the process length coming from the processor, wherein the forgoing inputted data is registered, and the register signal is outputted to the format device of the processor by the second storage unit.

14. The programmable data processing apparatus of claim 13, wherein the format device will prioritize the second input coming from the second storage.

15. The programmable data processing apparatus of claim 13, wherein the second storage unit is a register.